

**AFFIDAVIT FOR SEARCH WARRANT**

I, Amy L. Chandler, a Special Agent (“SA”) with the Federal Bureau of Investigation (“FBI”), being duly sworn, depose, and state as follows:

1. I have been employed as a Special Agent with the FBI since April 11, 2010, and am currently assigned to the Minneapolis Division, Minot Resident Agency. My duties include, among other things, the investigation of violent crimes occurring within Indian Country. While employed by the FBI, I have investigated and participated in investigations involving federal criminal violations related to Innocent Images, child exploitation, human trafficking, sexual assault, and violent crimes. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.
2. Prior to being employed as a Special Agent with the FBI, I was an Assistant State Attorney for the 9<sup>th</sup> Judicial Circuit for Orange and Osceola Counties in Florida for more than four years. During that time, I reviewed, charged, and prosecuted criminal cases involving crimes against children, sexually based offenses, violent crimes, and drug offenses.
3. As a Federal Agent, I am authorized to investigate violations of laws of the United States, and to execute warrants issued under the authority of the United States.
4. I am submitting this affidavit in support of a search warrant authorizing a search of a white trailer labeled 213 located at 1465 Main S, Dickinson, North Dakota next to Koehler Communications and a storage unit located next to ABC Diesel at address 175 49 Avenue SW, Dickinson, North Dakota, Storage Unit 19 (the “subject premises”), and

is more particularly described in Attachment A, for the items specified in Attachment B hereto, which items constitute instrumentalities, fruits, and evidence of violations of Title 18, United States Code, Sections 2251, 2252, 2252A, and 2422, as more fully detailed herein. I am requesting authority to search the entire trailer and storage unit, and any computer, cell phones, and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

5. The statements contained in this affidavit are based in part on: information provided by other agencies; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the results of physical surveillance conducted by law enforcement agents; independent investigation; and my experience, training and background as a Special Agent with the FBI. Because this Affidavit is being submitted for the limited purpose of establishing probable cause to believe that JUSTIN BICKLE committed the above-described offenses, I have not included every detail of the investigation. In addition, unless otherwise indicated all statements contained in this Affidavit are summarized in substance and in part.
6. As will be shown below, there is probable cause to believe that evidence of violations of Title 18, United States Code Sections 2251, 2252, 2252A, and 2422, as more specified in Attachment B, will be found in the premises more particularly described in Attachment A.

**LEGAL AUTHORITY**

7. Title 18 U.S.C. § 2251(a) and (e) prohibits a person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempts to do so.
8. Title 18, U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, or produced using a minor engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, or attempts to do so.
9. Title 18, U.S.C. § 2252A(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in Title 18, U.S.C. §2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such child pornography as produced using materials that had traveled in interstate or foreign commerce, or attempts to do so.
10. Title 18 U.S.C. § 2422(b) prohibits a person from using the mail or any facility or means of interstate or foreign commerce to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any

sexual activity for which any person can be charged with a criminal offense, or attempts to do so.

**DEFINITIONS**

11. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

- a. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- b. “Child Pornography,” as used herein, includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. See Title 18 U.S.C. §2252 and §2256(2).
- c. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See Title 18 U.S.C. 2256(5).
- d. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of

the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. (See Title 18 U.S.C. § 2256(2A)).

- e. “Minor” means any person under the age of eighteen years. (See Title 18 U.S.C. § 2256(1)).
- f. “Computer,” as used herein, is defined pursuant to Title 18 U.S.C. § 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”
- g. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- h. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they

work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- i. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items
- j. “Computer passwords and data security devices,” used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- k. “Internal Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, meaning an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

- l. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiches, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing), or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device.
- m. A hash value is a mathematical value generated by applying an algorithm to a computer file that is represented by a sequence of hexadecimal digits. Among computer forensics professionals, the hash value is generally considered to be a unique signature or fingerprint for a file.
- n. “Port numbers” in terms of computer networking and the Internet are used to transfer information over a network or the Internet between two applications and can be used to identify the senders and receivers of information.
- o. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the

Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an “email address,” an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records (“ISP records”) pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISP’s servers, and other information, which may be stored both in computer data format and in written or printed record format.

- p. “Domain names” are common, easy to remember names associated with an Internet Protocol address. For example, a domain name of [www.usdoj.gov](http://www.usdoj.gov)” refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards, from right to left, further identifies part of an



organization. Examples of first level, or top-level domains, are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second level names will further identify the organization, for example, usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

- q. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.
- r. “Electronic Communication Service” refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. (See Title 18 U.S.C. § 2510(15)).

**BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND E-MAIL**

12. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.
- b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are: reproduction, communication, distribution, and storage.
- c. Child pornographers can now convert photographs onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously

(through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e. “Instant Messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

- d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.
- e. The Internet and World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
- f. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer in most cases.

- g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e. by saving an e-mail as a file on the computer or by saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

#### **CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTOR**

- 13. I know from my training and experience as a Special Agent and former prosecutor that the following characteristics are prevalent among individuals who collect child pornography:
  - a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.
  - b. The majority of individuals who collect child pornography collect explicit materials, which may consist of photographs, magazines, motion pictures, video

tapes, books, slides, computer graphics, digital, or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless, fuel their sexual fantasies involving children.

- c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer, e-mail, bulletin boards, Internet relay chat, newsgroups, instant messaging, and other similar vehicles.
- d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.
- e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), telephone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained in the original medium from which they were derived, in

telephone books or notebooks, on computer storage devices, or on scraps of paper.

- f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and/or damage.
- g. Recent studies have shown that those who collect child pornography are more likely to be “contact offenders” with children. In a study published in the Journal of Abnormal Psychology, Vol. 15, No. 3, pp. 610-615, by Seto, Cantor, and Blanchard, titled “Child Pornography Offenses are a Valid Diagnostic Indicator of Pedophilia,” the authors concluded an interest in child pornography is a strong indicator of pedophilia. In December 2010, Seto, Hanson, and Babchishin published an article entitled “Contact Sexual Offending by Men with Online Sexual Offenses,” in Sexual Abuse: A Journal of Research and Treatment. This article was a meta-analysis of 24 studies of possessors of child pornography. In the studies that relied only upon subsequent arrests and/or convictions, the number of contact offenses with children ran from 4.6% to 13.3%. In the three studies in which the subjects participated in polygraph examinations, the percentages ranged from 32.3% to 84.5%, with the middle study finding 55.3%. In the remaining three studies in which relied only upon self-reporting, the numbers ranged from 32.8% to 57.4%. Each of the last three studies was unique. In Neutze, Seto, Schaefer, Mundt, & Beier, the subjects were in Germany. They had sought counseling on their own and were not referred by the criminal justice system. In the venue where the study was conducted, therapists were not legally

required to report the admissions of their subjects (36.5%). In Quayle & Taylor (2003), the number of subjects sampled was small (23) and had established good rapport with the therapists (47.8%). Finally, in Coward, Gabriel, Schuler, and Prentky (2009), the subjects reported anonymously (32.8%). In performing their statistical analysis of these studies, Seto, Hanson, & Babchishin concluded that more than 50% of those convicted of “possession only” admitted to at least one contact offense, when one relied on more than an arrest or conviction for a new offense.

### **BACKGROUND OF THE INVESTIGATION**

1. On or about March 22, 2018, at approximately 2:23 AM, law enforcement in McKenzie County received a 911 call in response to shots fired. Witnesses were later located by McKenzie County Sheriff's Office and interviewed. Witnesses reported they heard two to three gunshots around 2:30 AM. Law enforcement determined that JUSTIN JAMES BICKLE, date of birth XX/XX/1989, telephone number (701) 609-4469, was the person that called 911.
2. During the 911 call, BICKLE reported he had just been shot and was driving to the hospital. BICKLE stated there was a black dually pickup truck with a rack on it stopped on the side of the road. BICKLE reported he was shot in the leg when he was on his way to his aunt's house. BICKLE advised a female asked him to look under the hood of her vehicle and then a male grabbed him. This happened on a gravel road all the way north past the apartments that run east and west.
3. At approximately 3:44 AM, law enforcement from McKenzie County Sheriff's Office responded to McKenzie County Hospital and interviewed BICKLE prior to BICKLE

being transported to Trinity Hospital in Minot. BICKLE stated he left Dickinson, North Dakota at approximately 11:00 PM Mountain Time to drive to Watford City, North Dakota to stay with his aunt and uncle. BICKLE stated it took him approximately one and a half hours to get to Watford City. When BICKLE got to Watford City, he observed a dually pickup truck pulled off on the side of the road with the hood up. BICKLE stated the headlights and flashers were on and a female, possible KRISTINA RILL, waved him down. BICKLE stopped and parked his vehicle behind the pickup truck. BICKLE approached the truck on the driver's side and walked toward the front of the truck. When BICKLE got to the front of the truck, he heard a male voice. BICKLE and the male fought until BICKLE heard a bang and was in pain. Before BICKLE could return to his vehicle, the male and female got in the truck and left.

4. Law enforcement requested BICKLE's consent to search his cell phone. BICKLE stated he wanted to speak to an attorney in the morning.
5. Law enforcement attempted to locate the exact scene where BICKLE stated he was shot but could not locate it.
6. Law enforcement noticed the pants BICKLE was wearing when he claimed to be shot were inconsistent with what he told law enforcement. The pants did not have as much blood on them as they would have been had BICKLE been wearing them when he was shot. The pants also appeared to be cleanly sliced open and not ragged like they would be from a gunshot. BICKLE also did not have much blood on his hands when he arrived at the hospital. During subsequent interviews of BICKLE, he provided inconsistent accounts of what happened when he was shot. BICKLE also provided inconsistencies in the timeline of events he provided to law enforcement.



7. KRISTINA RILL was interviewed by law enforcement and reported that BICKLE was supposed to meet with several males to settle a drug debt.
8. Law enforcement observed social media posts made by BICKLE while he was at the hospital that showed he may have communicated with other individuals about the incident, specifically on Snap Chat, where BICKLE posted comments and pictures of his injuries.
9. BICKLE was on federal parole at the time of the shooting.
10. As a result of interviews conducted and the numerous inconsistencies provided by BICKLE during the investigation, McKenzie County Sheriff's Office believed the shooting may have occurred in a vehicle or at a different location than provided by BICKLE. On or about March 23, 2018, McKenzie County Sheriff's Office obtained a search warrant for BICKLE's black 2002 Chevrolet Silverado, vehicle identification number 1GCHK29192E177172, displaying North Dakota temporary registration permit 27911.
11. On or about March 23, 2018, McKenzie County Sheriff's Office also obtained a search warrant for BICKLE's iPhone SE, Model A1662, IMEI 356598081398763, to search for evidence of his travel plans, specifically global positioning data from the time BICKLE left Dickinson to the time he arrived at the hospital on or about March 22, 2018. The search warrant also permitted a search for photographs of any injuries BICKLE sustained, the use or possession of illegal narcotics, which the incident may have stemmed from, and the possession of any stolen property, which may have led to the incident, and the metadata of any such photographic evidence. The search warrant permitted a search for any communication via text message, email, Snap Chat, Facebook

Messenger, or any other social media platform BICKLE may have used to communicate with others about a meeting the day of the incident which would show who the potential suspects are and also for any messages in relation to an alleged drug debt and stolen property. The search warrant also allowed for a search for any phone calls, logs or other verbal communications made through other applications for the day of the shooting and the day prior, March 21, 2018, which may help determine who BICKLE was meeting.

12. On or about March 23, 2018, Watford City Police Department extracted the data from BICKLE's iPhone SE. The data extraction was provided to McKenzie County Sheriff's Office.

13. During a review of the extracted data, particularly in the Photos app which comes standard on the iPhone, law enforcement with the McKenzie County Sheriff's Office observed multiple images of what appeared to be child pornography. In the "Recently Deleted" folder of the Photos app, law enforcement observed numerous images of what appeared to be child pornography. Some of the images appeared to depict prepubescent females in various stages of undress or conducting various sexually explicit conduct. Below is a small sample of the photographs observed by law enforcement on BICKLE's iPhone:

- a. IMG\_0463.JPG/5003.JPG depicts a young female with braces, engaged in oral sex with male bodily fluids on her tongue.
- b. IMG\_0441.PNG/5003.JPG depicts a prepubescent female in a sexually compromising position.
- c. IMG\_0250.JPG depicts what appears to be a prepubescent female with a male touching her left breast and her left hand touching her vaginal area.

- d. IMG\_0426.GIF appears to show a prepubescent female undressing and then masturbating.
14. The images in the “Recently Deleted” folder appeared to have been erased from 15 to 24 days prior to the iPhone being extracted. Also located in the “Recently Deleted” folder were “selfie” pictures of BICKLE amongst the images depicting child pornography and child erotica.
15. During a review of BICKLE’s Facebook Messenger, accounts: 100019267878056 associated with user name J.J. BICKLE and justin.bickle.9, law enforcement observed messages BICKLE sent to a single mother of two young daughters who reside in Bismarck. The messages progressed over the course of days and BICKLE suggested the young girls should model but it is “risqué.” When BICKLE was asked why, BICKLE responded the photos are in provocative poses, the pay is substantial, and the photos are sent to Europe to be place on pay to click sites.
16. Law enforcement also observed what appears to be child pornography and/or child erotica in BICKLE’s iCloud/iMessage area of the phone and online which were not searched in detail.
17. On March 26, 2018, McKenzie County Sheriff’s Office executed a search warrant on BICKLE’s 2002 Chevrolet Silverado. A thumb drive and a black iPhone, Model A1549, IMEI: 352020076085952, locked with a six-digit pin, were located in the truck.
18. McKenzie County Sheriff’s Office contacted BICKLE’s probation and parole officer and learned that a law enforcement agency in Montana has a current case open against BICKLE for solicitation/luring of a minor using the Internet. The minor involved in that case is a 14-year-old female.

19. BICKLE was interviewed post-Miranda on March 26, 2018. BICKLE provided the passwords and usernames to several social media sites and email addresses. BICKLE also stated he has a white Dell laptop computer that is either located at a trailer or storage unit in Dickinson, North Dakota. BICKLE advised law enforcement the storage unit is next to ABC Diesel in Dickson, North Dakota. BICKLE advised the trailer where the laptop may be located is a white trailer with a door on each side of the trailer and located in a lot next to Koehler Communications. BICKLE indicated he has only had his iPhone since about March 15, 2018.
20. On or about April 2, 2018, Dickinson Police Department verified with the storage unit located at 175 49 Ave SW, Dickinson, North Dakota, which is located right next to ABC Diesel, that BICKLE's mother, MICKI HALLGREN, rents storage unit number 19. The employees at the storage unit were also familiar with BICKLE frequenting the storage unit.
21. On or about April 2, 2018, Dickinson Police Department located a white trailer located next to Koehler Communications located at 1465 Main S, Dickinson, North Dakota, #213.
22. Law enforcement also found the cell phone that BICKLE called 911 from the night of the shooting. BICKLE left that phone with a friend. BICKLE told law enforcement they could take that cell phone. BICKLE told law enforcement there was not a passcode on the cell phone, but the phone was locked when the phone was recovered from BICKLE's friend. The cell phone seized by law enforcement was a Samsung Model SM-S327VL (GP) with IMEI: 355744091702369.

23. On or about March 27, 2018, McKenzie County Sheriff's Office contacted the FBI and requested assistance in the investigation.

24. On or about April 3, 2018, Detective Patrick Jones with the Perrysburg Police Department in Ohio provided information to SA Chandler pertaining to BICKLE. In or about January and February 2017, BICKLE contacted an 11-year-old female using Facebook account J.J. BICKLE. During the conversation, the minor child told BICKLE that she was only 11 years old. BICKLE told the child, "You can't send me any naughty pics or anything. Just so u know. I could get in trouble." The minor child asked BICKLE, "And why would I do that??? I have a boyfriend anyways." BICKLE responded, "Lol cuz hot little girls do weird shit." BICKLE asked the minor child to send pictures. BICKLE then messages the child, "U do something to me. I wanna show you but you'll be a meany head n wouldn't understand." The child asks, "Okay my twin said we will be nice so what do you mean...oh and sorry for that." BICKLE replied, "You turn me on? You know what that means?" The child responded, "Nope." BICKLE wrote, "Video chat me and I'll show you." The child responded, "I'm scared too." BICKLE told the child, "Don't be scared sweetie. It's normal and I'm really nice." The child replied, "um..." BICKLE told the child, "It's just normal stuff for life and you're getting old enough to know it. You don't want everyone else in your class knowing about it and you not." It then appears from the messages that BICKLE had video chats with the minor child. BICKLE later starts communicating with the child's twin sister. BICKLE continues to ask the minor child for pictures. When the child sends a picture of herself from the neck down fully clothed, BICKLE writes her, "Cute. Show me more." The child then sent a picture of herself from the neck down in what appears to be a two-

piece bathing suit. The child later writes BICKLE, "...there is nothing to do right now." BICKLE tells the child, "Do me lol." BICKLE then tells the child, "You can take some pics on the bed silly." BICKLE later sends a picture that he describes as a picture of him in boxers where the outline of his penis is visible and he is touching his penis on the outside of his boxers. BICKLE also messages the child, "7013003356."

25. On or about February 21, 2018, the minor child's parents reported the messages to law enforcement in Ohio after they discovered the messages in the child's Facebook Messenger account. The minor child reported to law enforcement that BICKLE also communicated with her using the TextNow app. BICKLE contacted the child on the TextNow app using telephone number (701) 300-3356.
26. On or about April 4, 2018, McKenzie County Sheriff's Office provided messages sent by BICKLE since his arrest. BICKLE messaged his mother on March 27, 2018, "This is a fucked up deal. Just fyi. They gunna raid trailer and storage unit. Mom. This is justin."

#### **SEARCH METHODOLOGY TO BE EMPLOYED**

27. To search for electronic data contained in computer hardware, computer software, and/or memory storage devices, the examiners will make every effort to use computer forensic software to have a computer search the digital storage media. This may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
  - a. Searching for image files to locate images of children engaging in sexually explicit conduct, examining log files associated with the receipt, transmission, and viewing of such images, and examining all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data

and determine whether that data falls within the items to be seized as set forth herein;

- b. Surveying various file directories and the individual files they contain;
- c. On-site triage of computer system(s) to determine what, if any, peripheral devices and/or digital storage units have been connected to such computer system(s), as well as a preliminary scan of image files contained on such system(s) and digital storage device(s) to help identify any other relevant evidence and/or potential victim(s);
- d. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- e. Examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- f. Scanning storage areas;
- g. Performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- h. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

### **ABILITY TO RETRIEVE DELETED FILES**

28. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files or remnants of deleted files may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recover” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files and the files are only overwritten as they are replaced with more recently-viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on the particular user’s operating system, storage capacity, and computer habits.

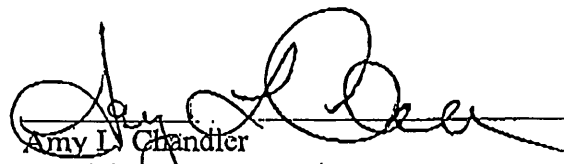
### **CONCLUSION**

29. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that JUSTIN JAMES BICKLE is involved in the possession of child pornography in violation of Title 18 U.S.C. Title 18, United States




Code, Sections 2251, 2252, 2252A, and 2422. Additionally, there is probable cause to believe that evidence of the commission of criminal offenses, namely, violations of Title 18 U.S.C. Title 18, United States Code, Sections 2251, 2252, 2252A, and 2422, are located within a white trailer with a door on each side of the trailer and located in a lot next to Kochler Communications at address 175 49 Ave SW, Dickinson, North Dakota, as well as a storage unit facility which is located right next to ABC Diesel, in storage unit number 19 at 1465 Main S, Dickinson, North Dakota, #213.

30. Therefore, I respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

  
Amy L. Chandler  
Special Agent  
Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED

BEFORE ME THIS 5<sup>th</sup> DAY OF APRIL, 2018, *telephone conference.*

  
Charles Miller  
United States Magistrate Judge